

Nursing

As you know, the nursing profession is under more pressure than ever before. And now, with the new HIPAA law, we have another topic we must master.

The HIPAA privacy regulations make big changes in the way we use information to care for our patients. They also give patients new rights over their own health information. We will need to know these new rights in order to help our patients.

As a nurse, you are your patients' best advocate for health issues. Now you will learn a set of guidelines to help you to be an advocate for their privacy as well.

Q: Does the HIPAA law mean we have to change about what we tell respiratory therapists and other nurses about our patients?

A: No, an important point is that the **minimum necessary disclosure** standard does not apply in treatment situations. That means you can freely share information with other caregivers as you've always done while keeping in mind your professional responsibility to consider what the other caregivers need to know.

Family Discussion and Opt-Out

Opt-out applies to disclosures of PHI to the family and friends involved in a patient's healthcare and to the use of information in facility directories. The patient has the opportunity to refuse, or opt out of, this type of disclosure.

The law says that you can make information disclosures to family, close friends or personal friends if you can reasonably infer from the circumstances that the individual would not object to the disclosure — so, in the end, use good judgment.

The Minor

Minors can present a more complicated privacy problem. The HIPAA regulations defer to all state laws regarding the disclosure of a minor's PHI, so you must know the rules for your state

The minor has the authority to act as his or her own individual in any of the following situations:

- If the minor is allowed by state law to consent to the healthcare service, has consented, and has not designated a personal representative.
- If the minor may receive the healthcare service by law without consent.
- If the parent or guardian consents to agreement of confidentiality between the minor regarding health information and us.

Patients With Dementia

We see many patients who have dementia these days. Managing the PHI of your dementia patients requires your best professional judgment.

You can disclose health information about the patient to someone who:

Has power of attorney for the patient.

Cares for the patient and brought the patient to the healthcare facility.

For a patient with early, mild dementia, use professional judgment to decide whether the patient understands the issues involved in opting in or opting out of family disclosures.

Opting Out of a Facility Directory

A patient can also opt out of having PHI information listed in a facility directory. When someone is admitted to the facility, you should ask the patient, "Do you mind if we list you in our facility directory?"

The following items can be put in a facility directory:

- Name
- Location
- Condition, in general terms
- Religious affiliation

If a patient opts out, do not list the patient's name in the facility directory. The facility directory does not contain diagnosis or other specific information.

Being Included in a Facility Directory

We inform the patient who does **not** opt out that being included in the facility directory means that we give this information to:

- Anybody who asks for the patient by name.
- Any clergy associated with the patient's religious affiliation.

Questions and Answers

Q: What about whiteboards? I've heard we're not allowed to keep patient information on whiteboards any more.

A: The important thing is the location of the whiteboard. Keep it away from areas where the general public can see it. If viewing by visitors is unavoidable, you must make your best effort to conceal the individually identifiable health information on the board. Use initials for patient names and code words for their diagnoses or procedures. The rule is that we make our best effort not to have people's private information posted on whiteboards where outsiders can see it.

Q: Do I have to take patients into private rooms now to take a history?

A: No, shared rooms are common in hospitals. The emergency department isn't very private at all. Just remember, when you take a history from your patient, do what you can to protect your patient's privacy. Take such actions as:

- Closing the curtains.
- Speaking in a low volume so others don't overhear you.

Use your best professional judgment!

Q: What about the clutter at the nursing station?

A: Don't leave patient information; such as nursing care sheets, progress notes, or vital sign charts, open and easily viewable in accessible areas like the nursing station. Information left in patient rooms should be covered to protect confidentiality. You are your patient's advocate. Protect their PHI.

Q: What do I do if a patient tells me she wants to revoke an authorization she signed the last time she was in?

A: Let her know that you will pass her wishes on to medical records. Then notify medical records of the patient's wish to revoke the authorization. Be sure to provide information regarding what the authorization was for, in case there is more than one authorization in the patient's file.

Knowing how HIPAA and our organization expect you to handle patient PHI and how to answer questions about our patients is important for all of us.

Protected Health Information

Use this easy decision device to determine if medical information qualifies as PHI.

1. Does the information identify an individual or is there a reasonable basis to believe that the information can be used to identify the individual? *If yes, proceed to #2.*
2. Does the information relate to the past, present, or future physical or mental health or condition of an individual or the provision of health care to that individual or the past present or future payment for the provision of health care to an individual? *If yes, proceed to #3.*
3. Was the information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse? *If yes, proceed to #4.*
4. Is the information education records or post-secondary student medical records that are covered in the Family Educational Right and Privacy Act or 20 USC 1232g(a)(4)(B)(iv), or is the information employment records held by a covered entity in its role as an employer?

Only health information that identifies an individual is subject to the HIPAA privacy rule. Health information that could not be reasonably used to identify an individual is not subject to the privacy rule and can be freely disclosed.

Health information can be “de-identified” by removing all of the following identifiers regarding the individual, relatives, employers, or household members:

- Names
- Geographic subdivisions
- All elements of dates
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account Numbers
- Certificate/license numbers
- Health plan beneficiary numbers
- Account numbers
- Vehicle identifiers
- Device identifiers and serial numbers
- Web Universal Resource Locator (URL)
- Internet protocol (IP) address number
- Biometric identifiers
- Full-face photographic images
- Any other unique identifying number, characteristic or code

Verifying the Requester/Minimum Disclosure

Patients have been notified that we will use their information in day-to-day business. But we have to be **careful** with people’s health information. The two key principles of being careful with health information are:

- Verifying the requester
- Disclosing only minimum necessary information

Verify Requester

To verify the requester we must verify both the **identity** and the **authority** of the person requesting information.

Verify Identity

There are many ways to verify that people are who they say they are:

- Ask for a birth date or social security number
- Ask for the mother’s maiden name or some other unique information
- Check a physical signature against a known one on file, or
- Make a call back to a known number

Verify Authority

Once you know who the requester is, verify that he or she has the right to access this information.

Routine request from employees you know in your own organization are usually OK.

You must verify both the identity and the authority of the requester to be sure you can disclose protected health information.

Even after we have verified the requester, we must disclose **minimum necessary information** to take care of PHI.

Once you are comfortable with the requester, give out only what the person really needs to know. Our co-workers will usually only ask for what they need. Unusual requests from individuals you don't know are risky. Limit the information you give out—no more than **exactly** what they are authorized to receive!

We need to be careful with people's health information. People expect that we will protect their information from anyone who does not need to know it, even our own employees.

Our organization has specific policies and procedures to help you decide how to make or request disclosures in your daily work. Be sure you know the policies that apply to you.

If you are in doubt, or something doesn't feel right, ASK! You must go to your supervisor or privacy officer for help.

Damage Control

Our organization is committed to making sure that individuals are not harmed by the unauthorized disclosure of their protected health information.

What should you do if you learn that private health information has been released outside of routine business functions, without authorization?

Tell your supervisor, or the privacy officer! We have a duty to **MITIGATE THE EFFECTS** of unauthorized release.

This is to certify that I, _____ have read and understand all policies and guidelines governing the HIPAA regulation.

Signature

Date